Context

"It's personal. It's private. And it's no one's business but yours." This is how Phil Zimmermann, the author of the popular PGP program[1], summarizes the many reasons why we should encrypt data. We at Jamcracker believe that this is true especially in our very competitive area.

Description of Information:

1. **Public Information**: Data of this type could be made public without any implications for the company (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger. Examples: Test services without confidential data, information held on certain public servers or a picnic invitation.

2. **Internal Information** : External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. at worse, the company may be publicly embarrassed). Internal access must be somewhat restricted. Data integrity is important but not vital. Examples of this type of data are found in development groups (where no live data is present), certain production public services, certain Customer Data, "normal" working documents and project/meeting protocols as well as internal telephone books.

3. **Confidential Information** : Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorized parties, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity is vital. Examples: salaries, personnel data, accounting data, very confidential customer data, sensitive projects and confidential contracts. Data centers normally maintain this level of security.

4. **Secret Information** : Unauthorized external or internal access to this data is detrimental to the company. Data integrity is vital. Access to this data must be limited to a very small number of people and must be controlled with very strict

[1] See the Web document entitled "Why do you need PGP?" by Phil Zimmermann at http://www.pgpi.org/doc/whypgp/en/

rules. Examples: information about major pending contracts/reorganization/financial transactions or application architecture data.

Guidelines

E-mail exchange

- Every e-mail sent to an internal Jamcracker recipient, such as employee or contractor, must be encrypted.
- Moreover, every internal, confidential or secret information sent to outside parties must be encrypted using a mutually agreed upon encryption method. PGP must be the preferred method.
- Secret information must be encrypted using a strong encryption method, as supplied by PGP. Encryption using weak schemes (.zip password or simple XOR must be avoided at all cost).

Storage of information

- Confidential information stored on the local hard disk of a desktop computer must be encrypted using a strong encryption algorithm. *PGPDisk* can be used for this purpose for information stored locally.
- Secret information stored on any local media, on the internal network or at any other location, must be encrypted at every stage of its life. When deleted, its former medium footprint must me wiped with the PGP *Wipe* function.
- Any non public information stored on the local hard disk of a **laptop computer** must be encrypted. Other encryption guidelines described above must also be applied.